INTERNET ASSOCIATION OF AUSTRALIA LTD
ABN 71 817 988 968
ACN 168 405 098
PO Box 8700
Perth Business Centre WA 6849
Phone: 1300 653 132

21 June 2024

To: Director – Strategy and Research
Online Safety, Media and Platforms Division
Department of Infrastructure, Transport
Regional Development, Communications and the Arts

GPO Box 594 Canberra, ACT 2601

By submission: https://www.infrastructure.gov.au/have-your-say/statutory-review-online-safety-act-2021

RE: Statutory Review of the Online Safety Act 2021

The Internet Association of Australia (**IAA**) thanks the Department of Infrastructure, Transport, Regional Development, Communications and the Arts (the **Department**) for the opportunity to respond to the consultation on the Statutory Review of the Online Safety Act 2021.

IAA is a member-based association representing Australia's Internet community. Our membership is largely comprised of small to medium sized Internet carriage service providers (**ISPs**). Some of our members may also provide other services, such as email services and telephony relevant electronic services. This response is therefore primarily in representation of such members. Furthermore, IAA appreciates the opportunity to engage in consultation as an association concerned with and committed to the public good of the Internet.

From the outset, IAA and our members hold online safety as being fundamentally important, particularly in today's digital age. We understand that most Australians' daily lives occur online, including children, and therefore, are committed to ensuring that the Internet is a safe environment.

However, we are also committed to effective regulation, and believe that legislative measures should instil practical solutions that target the appropriate entities, and minimises unnecessary burden on industry, and individuals. To that end, we emphasise the importance of continuing to ensure the distinction between different types of Internet-related service providers. Carriage service providers that are mere conduits, and do not supply 'Over the Top' or other content services, should have minimal requirements under any revised Online Safety Act 2021 (**OSA**), as has been generally recognised thus far.

We also advocate for evidence-based legislative reform, and believe this to be critical to ensuring an online safety regime that is actually beneficial for end-users of online services. As will be detailed in our response below, we are concerned that some proposals being considered in the Issues Paper do not provide sufficient data or information to support the proposed changes.

We therefore offer our recommendations and feedback in response to the questions posed by the Issues Paper below.

OUR RESPONSE

PART 2: AUSTRALIA'S REGULATORY APPROACH TO ONLINE SERVICES, SYSTEMS AND PROCESSES

2. ***Does the Act capture and define the right sections of the online industry?***
3. ***Does the Act regulate things (such as tools or services) that do not need to be regulated, or fail to regulate things that should be regulated?***
7. ***Should regulatory obligations depend on a service provider's risk or reach?***

We strongly support both the segmentation of the online industry as well as introducing a risk and/or reach approach.

Regarding industry segmentation, our members have noted that it is becoming increasingly difficult for ISPs to monitor what is being accessed by their customers due to use of new technologies. We also note that as outlined in Table 2.2 of the Issues Paper, the inclusion of ISPs in Australia's online safety regime seems to be novel in comparison to legislative regimes overseas. As such, any legislative reform should carefully consider which segments of the online services industry should bear certain responsibilities, and as much as possible, ISPs should continue to be recognised as serving as mere conduits, with relatively limited control over what material and activities are occurring online.

However, we also understand and agree that as technologies continue to evolve, it is difficult to appropriately segment the various services to ensure the applicable service providers are being subject to certain requirements. For example, some of our members may also be captured as providing 'relevant electronic services' due to its broad definition. As such, we would support the adoption of the UK approach of using the risk and reach model, in conjunction with the industry segmentation, particularly when it comes to the proposed introduction of a statutory duty of care, as well as the Phase 2 Codes. That is, Australia's online safety legislative regime should be amended so that provisions are specific and proportionate to the type of online services provided by an entity, as well as a service provider's reach and potential risk posed to end users.

4. ***Should the Act have strengthened and enforceable Basic Online Safety Expectations?***

We are concerned that making the BOSE enforceable would result in greater confusion and a potentially duplicative regulatory regime. We note the current existence of the OSA, and the industry codes and standards under the Online Content Scheme, as well as the reputational incentive and pressure for service providers to comply with the BOSE. The Issues Paper has not provided sufficient evidence or information to indicate it is necessary or would be beneficial to make the BOSE enforceable.

If making the BOSE enforceable is pursued, we would recommend repealing the BOSE altogether and instead incorporate it into the OSA, to avoid any confusion for individuals and service providers about their respective rights and responsibilities. However, in such a case, this requires further consultation to ensure that any new provisions are appropriate and subject to other considerations such as the application of the reach and risk principle as discussed above.

We also note that the BOSE has been recently reviewed and amended. Arguably, it is now strengthened to include enhanced protection for individuals, particularly children.

PART 3: PROTECTING THOSE WHO HAVE EXPERIENCED OR ENCOUNTERED ONLINE HARMS

9. ***Are the complaints schemes accessible, easy to understand and effective for complainants?***

Due to the various schemes that exist, it is not sufficiently accessible or easy for not only complainants and end users to understand their rights and responsibilities, but also service providers. We appreciate the webform made available on the eSafety website that assists complainants in understanding the type of online harm, and therefore the appropriate course of action to be taken. We would recommend a similar matrix or guidance material be developed for service providers to help them understand what their obligations are under each scheme, and for online safety related legislation. This will result in increased compliance, and therefore, better outcomes for individuals, including those seeking to access complaint mechanisms.

16. ***What more could be done to promote the safety of Australians online, including through research, educational resources and awareness raising?***

We advocate for a holistic and whole of ecosystem approach to research, education and awareness. As stated above, we believe more awareness and educative material is needed for both industry and individuals. Given the rapidly evolving online industry, there are many smaller and emerging digital platforms and service providers that do not have the same resources to understand and unpack regulation as is the case for larger entities. Improving awareness within the industry is critical to ensure better protections for individuals. Furthermore, greater collaboration with the Department of Education, as well as State and Territory governments to ensure online safety is being taught at all schools from a young age is necessary.

PART 4: PENALTIES, AND INVESTIGATION AND INFORMATION GATHERING POWERS

17. ***Does the Act need stronger investigation, information gathering and enforcement powers?***
18. ***Are Australia's penalties adequate and if not, what forms should they take?***

We understand that the Department is considering increasing penalties to reflect penalty regimes in place in other jurisdictions. However, the Issues Paper does not provide sufficient evidence as to whether such higher penalties have resulted in better outcomes. Conversely, Part 3 of the Issues Paper suggests that in most cases where the eSafety Commissioner made or issued a removal request or notice, such requests or notices were successful, and has not otherwise suggested there is a significant problem with non-compliance in Australia to justify increasing penalty amounts.

It is our understanding that in other legislative regimes such as Australian consumer law, or privacy law, penalty amounts were increased to serve as greater deterrents due to the issue of businesses simply regarding 'low' penalty amounts as acceptable costs of doing business. This

does not seem to be the case based on the Issues Paper.

It seems unnecessary to increase penalties for the sake of matching penalty regimes that are applied in other jurisdictions. If increased penalties are being seriously pursued by the Department, there should be further research and analysis conducted to assess whether the establishment of higher penalties has resulted in better outcomes such as service providers being more proactive in implementing mechanisms to protect individuals from online harm, whether such penalties have been used to provide direct and practical redress for individuals negatively impacted by online harm, or actually serve as a stronger deterrence for end users propagating harmful material.

Furthermore, at the least, increased penalties should be proportionate to the seriousness of the harm to the individual, as well as the size and reach of the service provider. As noted in the Issues Paper, penalty amounts could be amended to ensure proportionately higher amounts for systematic or egregious non-compliance. However, it is important that we strongly oppose the suggestion in the Issues Paper that failure to comply with an industry code is evidence of 'systematic non-compliance', which would then warrant higher penalties. While we understand the intent of the distinction made in the Issues Paper, it is important to note that not all requirements under the industry codes or standards have the same risk level. Furthermore, as stated above, there is a need for increased awareness amongst industry to assist particularly small and under-resourced service providers with their regulatory compliance. Where a service provider mistakenly does not comply with an industry code or standard and corrects this non-compliance upon being notified, as opposed to a service provider's contumelious disregard of online safety laws, to apply higher penalties based on an arbitrary distinction that non-compliance with a code represents a systematic issue would be unfair. Rather, it may be more appropriate to consider whether non-compliance is repeated, to warrant high penalties.

19. ***What more could be done to enforce action against service providers who do not comply, especially those based overseas?***
20. ***Should the Commissioner have powers to impose sanctions such as business disruption sanctions?***

We appreciate the efforts of the Department and the eSafety Commissioner in dealing with service providers based overseas to ensure the protection of individuals. However, we are concerned about the potential adverse effects of introducing a business disruption sanction measure in Australia to combat the difficulties of enforcement against overseas service providers. This is likely to unintentionally have adverse effects on end users, including small businesses in Australia that rely on social media and other online services for their business. Furthermore, this may also be difficult to enforce due to the use of VPNs and other technologies to still access services sanctioned in Australia, and would also result in further complexities as new laws would have to be developed to ensure other entities such as payment providers, advertisers and ISPs do not work with the sanctioned service provider. It would also result in the fragmentation of the Internet, which is not to the benefit of individuals in Australia. This seems to oppose the principle of a public and open Internet which we support as best practice.

Rather, it seems that enforcement with respect to overseas providers is an issue that should be considered on a global level, with input from regulators overseas as well as industry and service providers. We understand that the Global Online Safety Regulators Network was recently established; we would recommend the Network engage with online service providers to devise a

harmonious, measured and appropriate enforceability scheme that would apply in each jurisdiction.

PART 5: INTERNATIONAL APPROACHES TO ADDRESS ONLINE HARMS

21. ***Should the Act incorporate any of the international approaches identified above? If so, what should this look like?***
22. ***Should Australia place additional statutory duties on online services to make online services safer and minimise online harms?***

As mentioned above, the BOSE was recently amended to enhance protections for individuals, including requiring service providers to take reasonable steps to ensure the best interest of the child. While we understand the BOSE is not enforceable, we believe such reforms will result in better protections. We would therefore recommend further research such as analysis of the results and outcomes of measures introduced overseas prior to adopting them in Australia, as well as review the effectiveness of the recently amended BOSE, prior to introducing additional statutory duties.

24. ***Should there be a mechanism in place to provide researchers and eSafety with access to data? Are there other things they should be allowed access to?***

We understand that reporting requirements already exist to provide information to eSafety. We do not believe that sufficient information has been provided in the Issues Paper to explain what sort of data eSafety is seeking access to, and for what purpose. We also note that introducing a requirement that allows regulators and researchers to access data has privacy implications and is not necessarily in the individual's interest. Furthermore, it would also result in great costs to service providers, particularly smaller providers, to develop systems to allow such access to data, especially in ways to ensure minimal infringement to end users' privacy, as well as protections for their confidential business data.

Given these potential costs and harms (and others not specified above), we believe it would be prudent to provide further information and evidence as to what would be achieved and the potential benefits that would flow from allowing such access to data. Although we understand that in some overseas jurisdictions, service providers are being required to provide access, the Issues Paper does not seem to consider what the outcomes of such powers have been, and whether they represent net positives for individuals and the broader Internet industry and ecosystem.

PART 6: REGULATING THE ONLINE ENVIRONMENT, TECHNOLOGY AND ENVIRONMENTAL CHANGES

29. ***Should the Act address risks raised by specific technologies or remain technology neutral? How would the introduction of a statutory duty of care or Safety by Design obligations change your response?***

We strongly support keeping the OSA technology neutral. Specific technologies may be dealt with via guidance material, or where appropriate and necessary, via the industry codes and standards. Moreover, if a statutory duty of care or Safety by Design obligations are introduced, we believe this can still be principles based in the legislation to allow flexibility for service providers, as well as reducing the likelihood of legislation soon becoming obsolete.

31. ***What features of the Act are working well, or should be expanded?***

We support the continuation of the co-regulation model of industry designed codes, and would support its expansion to introduce any new requirements in addition to the Phase 2 Codes. We also support the hybrid approach of having both systemic requirements on online service providers, while also allowing for individual complaint mechanisms. However, as discussed above, we would recommend amendments to incorporate the proportionate risk and reach approach to better target appropriate service providers.

32. ***Does Australia have the appropriate governance structures in place to administer Australia's online safety laws?***

We recommend the adoption of the UK approach so that the eSafety Commissioner's office is governed by a board that can provide strategic direction and develop terms of reference as well as improve transparency and oversight.

CONCLUSION

Once again, IAA appreciates the opportunity to contribute to the Statutory Review of the Online Safety Act 2021. IAA and our members are greatly invested in the development of a healthy, thriving and safe online environment. To that end, we are deeply committed to working with the Department, eSafety and other regulators, as well as civil society and other relevant stakeholders to ensure effective and appropriate legislative reform.

ABOUT THE INTERNET ASSOCIATION OF AUSTRALIA

The Internet Association of Australia (IAA) is a member-based association representing the Internet community. Founded in 1995, as the Western Australian Internet Association (WAIA), the Association changed its name in early 2016 to better reflect our national membership and growth.

Our members comprise industry professionals, corporations, and affiliate organisations. IAA provides a range of services and resources for members and supports the development of the Internet industry both within Australia and internationally. Providing technical services as well as social and professional development events, IAA aims to provide services and resources that our members need.

IX-Australia is a service provided by the Internet Association of Australia to Corporate and Affiliate members. It is the longest running carrier neutral Internet Exchange in Australia. Spanning six states and territories, IAA operates over 30 points of presence and operates the New Zealand Internet Exchange on behalf of NZIX Inc in New Zealand.

IAA is also a licenced telecommunications carrier, and operates on a not-for-profit basis.

Yours faithfully,

Narelle Clark
Chief Executive Officer
Internet Association of Australia